AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

Claims 1 to 3. (Canceled)

4. (Previously Presented) A method for generating, personalizing, and certifying an asymmetrical cryptokey in accordance with one of an operation performed at a central, secure location corresponding to a trust center and an operation performed at a user location in cooperation with the trust center using a secure transmission between a user and the trust center, the method comprising the steps of:

causing the trust center to provide the user with a previously generated, personalized, and certified signature key pair, and with components for producing at least one encryption key pair;

producing by the user the at least one encryption key pair including a public part and a secret part;

marking the public part of the at least one encryption key pair using an assigned secret part of the previously generated signature key pair;

after marking the public part of the at least one encryption key pair, transmitting the at least one encryption key pair to the trust center;

unequivocally assigning the at least one encryption key pair to the user;

causing the trust center to check the unequivocal assignment of the at least one encryption key pair by using a public part of the previously generated signature key pair;

after the check of the unequivocal assignment is performed successfully, causing the trust center to produce a new certificate by using at least one of the public part of the previously generated signature key pair and the public part of the at least one encryption key pair;

encrypting the new certificate using the public part of the at least one encryption key pair; and

causing the trust center to transmit the encrypted new certificate to the user.

5. (Previously Presented) The method according to claim 4, wherein:

the step of causing the trust center to provide the user with components for producing at least one encryption key pair includes the step of providing the user with components for producing at least one additional signature key pair,

the step of producing the at least one encryption key pair includes the step of producing the at least one additional signature key pair, and

the user marks a public part of the at least one additional signature key pair

using the secret part of the previously generated signature key pair.

6. (Previously Presented) The method according to claim 5, further comprising the steps of:

in each bilateral communication occurring between a user desiring no communication with the trust center and another user, marking and making available to the other user one of the public part of the at least one encryption key pair and the public part of the at least one additional signature key pair by using the secret part of the previously generated signature key pair; and

checking a correctness of an assignment regarding one of the public part of the at least one encryption key pair and the public part of the at least one additional signature key pair by performing the steps of:

verifying a signature, and

checking a genuineness and a validity of the new certificate in the trust center.

7. (Previously Presented) A method for generating, personalizing, and certifying an asymmetrical cryptokey in accordance with one of an operation performed at a central, secure location corresponding to a trust center and an operation performed at a user location in cooperation with the trust center using a secure transmission between a user and the trust center, the method comprising the steps of:

causing the trust center to provide the user with a previously generated, personalized, and certified signature key pair, and with components for producing at least one encryption key pair;

producing by the user the at least one encryption key pair including a public part and a secret part;

marking the public part of the at least one encryption key pair using an assigned secret part of the previously generated signature key pair;

after marking the public part of the at least one encryption key pair, transmitting the at least one encryption key pair to the trust center;

unequivocally assigning the at least one encryption key pair to the user;

causing the trust center to check the unequivocal assignment of the at least one encryption key pair by using a public part of the previously generated signature key pair;

after the check of the unequivocal assignment is performed successfully, causing the trust center to generate a new certificate by using one of: i) the public part of the previously generated signature key pair and the public part of the at least one encryption key pair, and ii) the public part of the at least one encryption key pair;

encrypting the new certificate using the public part of the at least one encryption key pair;

causing the trust center to transmit the encrypted new certificate to the user;

in each bilateral communication occurring between a user desiring no communication with the trust center and another user, marking and making available to the other user the public part of the at least one encryption key pair by using the secret part of the previously generated signature key pair; and

checking a correctness of an assignment regarding the public part of the at least one encryption key pair by performing the steps of:

verifying a signature, and

checking a genuineness and a validity of the new certificate in the trust center.

8. (Previously Presented) The method of claim 4 wherein the secret part of the encryption key pair is not revealed by the user.

9. (Previously Presented) The method of claim 7 wherein the secret part of the encryption key pair is not revealed by the user.